Journal of Environmental Protection and Ecology 25, No 5, 1361–1370 (2024)

Risk assessment

USE OF BLOCKCHAIN FOR IoT APPLICATIONS, PLATFORMS, SYSTEMS, AND FRAMEWORKS

K. M. VEERABHADRASWAMY[a]*, M. D. SIVA RANJANI[b], WARISH PATEL[c], M. V. RAMA SUNDARI[d], KSHITIJ NAIKADE[e], RUHI BAKHARE[f], L. ANBARASU[g], R. PREMANAND[h], A. RAJARAM[i]

[a]*Department of Electronics and Communication Engineering, Government Engineering College, Mosalehosahalli, 573 212 Hassan, Karnataka, India*
E-mail: *veerabhadraswamy6790@gmail.com*
[b]*Department of Computer Applications, Mepco Schlenk Engineering College, 626 005 Sivakasi, Tamil Nadu, India*
[c]*Department of Computer Science and Engineering, Parul Institute of Engineering and Technology, Parul University, 391 760 Gujarat, India*
[d]*Department of Artificial Intelligence and Machine Learning, Gokaraju Rangaraju Institute of Engineering and Technology, 500 090 Telangana, India*
[e]*Faculty of Law, Symbiosis Law School (SLS) Symbiosis International (Deemed University) (SIU), Vimannagar, 411 014 Pune, Maharashtra, India*
[f]*Dr. Ambedkar Institute of Management Studies and Research, 440 010 Nagpur, Maharashtra, India*
[g]*Department of Electrical and Electronics Engineering, Erode Sengunthar Engineering College, 638 057 Erode, Tamil Nadu, India*
[h]*Department of Humanities and Science (Physics), Sri Sai Ram Engineering College, 600 044 Chennai, Tamil Nadu, India*
[i]*Department of Electronics and Communication Engineering, E.G.S. Pillay Engineering College, 611 002 Nagapattinam, Tamil Nadu, India*

Abstract. In the realm of the Internet of Things (IoT), the integration of blockchain and distributed ledger technologies offers promising avenues for establishing secure and trustless solutions. However, the prevailing insecurity of IoT devices necessitates blockchain-based solutions to not only mitigate existing challenges but also avoid introducing new vulnerabilities, particularly performance issues hindering adoption. This paper addresses these imperatives by comprehensively reviewing available blockchain solutions with a focus on the industrial domain. The study scrutinises key architectural aspects of blockchain systems, including software platforms, network configurations, consensus protocols, and smart contracts, in terms of their resilience against common IoT and blockchain attacks, provision of enhanced privacy features, and ability to maintain performance amidst IoT transaction volumes. The analysis reveals that while blockchain platforms exhibit varying degrees of resilience against attacks, with blockchain 1.0 and 2.0 platforms being particularly susceptible, they

* For correspondence.

demonstrate some support for privacy features. However, the assessment of overall privacy remains complex due to platforms addressing specific aspects. Considering performance and fault tolerance of underlying consensus protocols, only a limited number of platforms meet the requirements for industrial IoT scenarios. This review underscores the need for robust blockchain solutions tailored to the unique challenges of IoT applications, particularly in industrial settings, to ensure the integrity, security, and efficiency of IoT systems.

Keywords: blockchain, Internet of Things, security, consensus protocols, software platforms, network configurations, smart contracts.

AIMS AND BACKGROUND

Blockchain technology and the Industrial Internet of Things (IIoT) have great potential to transform industrial processes by enabling networks that are safe, smart, and self-governing[1]. The Internet of Things (IIoT) enables the connecting of several stakeholders and devices, leading to sophisticated industrial applications with strict security, performance, and trust requirements[2]. Blockchain solves these issues by guaranteeing data consistency, security, and interoperability as a distributed and decentralised ledger[3]. Data management, security, and reliability can all be improved for different businesses by incorporating blockchain into IIoT platforms. Heterogeneity, interoperability, and single points of failure in conventional IIoT networks are among the issues that this integration helps to address[4]. A redundant, traceable, and secure environment is provided for intricately coupled IIoT systems by the coupling of IIoT and blockchain, also known as Blockchain for Industrial Internet of Things (BIIoT). Reliability and efficiency in industrial processes are improved by BIIoT, which enables decentralised communication and does away with the need for reliable middlemen[5]. Realising the potential of Industry 4.0, where automation and digitisation play major roles in fostering industrial innovation and competitiveness, depends on this integration. Numerous scholarly investigations have examined the capacity of blockchain technology to transform industrial applications. It was highlighted[6] how blockchain can control access on a worldwide scale, offering a granular way to monitor transfers and network logs, guaranteeing anonymity and uniformity across different sectors. Overview[7] of blockchain's fundamental characteristics and its potential to secure Internet of Things (IoT) under Industry 4.0 included recommendations for blockchain-based IoT applications. In their investigation of use cases like supply chains and healthcare, the authors[8] outlined strategies to get around barriers and improve blockchain adoption for IoT. In the analysis of blockchain innovations in eHealth and smart cities, some authors[9] addressed knowledge gaps and offered fog computing solutions. Blockchain-enabled Internet of Things (IoT) security achievements and problems were evaluated[10], who also identified important applications and future research objectives. In their discussion of blockchain security risks, suggestions for improving blockchain security measures[11] were offered. Numerous research works emphasise how blockchain technology can be integrated with industrial

technologies to improve automation, productivity, and safety. A Blockchain-enabled Safety-as-a-Service (Safe-aaS) system is proposed[12] to enhance on-site safety by offering personalised safety choices and taking privacy issues into account. In order to solve issues like decentralisation and security vulnerabilities, Dwivedi et al.[13] explore Industry 4.0's integration with IoT and blockchain, paying particular attention to data storage, smart contracts, and technological convergence. Blockchain applications in Industrial IoT (IIoT) and supply chain systems are reviewed by Malik et al.[14], who highlight the technology's advantages for improving security and integrity. Yang et al.[15] introduce EdgeShare, a blockchain-based data-sharing framework for IIoT, enhancing efficiency and security through edge computing and smart contracts. These studies collectively underscore the potential of blockchain technology in addressing challenges and enhancing various aspects of industrial processes, safety, and data management.

EXPERIMENTAL

IDENTIFICATION OF CHALLENGES

Numerous scholarly works tackle the difficulties associated with incorporating cutting-edge technology such as blockchain and the Industrial Internet of Things (IIoT) into diverse industrial sectors. Li et al.[16] point out challenges in applying blockchain to Supply Chain Quality Management (SCQM), such as managing privacy and trust issues, transferring to blockchain systems, managing huge datasets, and effectively storing referral data. The issues of assuring security and privacy in the context of the Internet of Things are outlined by Gebremichael et al.[17] These challenges include preventing privacy breaches, reducing security threats, resolving infrastructure compromise, and guaranteeing availability, confidentiality, and integrity. Serror et al.'s discussion[18] of IIoT security challenges centres on safety and productivity needs, reliability and data integrity assurance, and handling the intricacy of networks and devices that are interconnected. These studies highlight the necessity for creative approaches to problems in order to improve the efficacy of blockchain and IIoT technology integration in industrial settings.

REVIEW OF BLOCKCHAIN SOLUTIONS

A comprehensive architecture that combines Security-by-Contract (S×C) protocols, MUD profiles, blockchain technology, and software-defined networking is presented by Krishnan et al.[19] for safeguarding IIoT devices in Industry 4.0 networks. This method uses MUD profiles for network functioning and behavioural profiles embedded in IoT devices to identify device capabilities, detect problems, and stop cyberattacks and misconfigurations. The IoT onboarding process integrates authentication techniques and uses blockchains as a verified repository to store network manifests and guarantee integrity. The COaaS framework is introduced by

Uriarte et al.[20], who use Hyperledger Sawtooth for cloud orchestration. Scalability and speed gains are provided via Sawtooth's modular architecture and support for pluggable consensus algorithms, especially PoET.

In order to automate transactions and guarantee secure data management in healthcare services, Khan et al.[21] implement smart contracts in the BIoMT system. In addition to creating a secure network and providing dynamic monitoring environments, these contracts handle tasks like device registration, data preservation, service requests, and ledger encryption. Blockchain alternatives for the industrial domain are reviewed by Gourisetti et al.[22], who concentrate on important architectural elements including software platforms, network setups, and consensus mechanisms. Highlighting advantages like machine-to-machine transactions and integration into grid operations for automated market bidding and resilient grid management, they place emphasis on leveraging blockchain attributes to address cybersecurity needs while facilitating market mechanisms in transactive energy systems. According to Lin et al.[23], smart contracts function autonomously in response to preset triggers, guaranteeing tamper-proof and transparent actions at all stage of their lifespan, including creation, release, and execution. Ethereum uses transactions to implement smart contracts. Solidity code is converted into EVM bytecode and then sent to the network through JSON-RPC interfaces. The execution of transactions costs gas. Hyperledger Fabric uses chaincode to encapsulate business logic and is deployed as stand-alone containers. The deployment procedure includes constructing Fabric networks, deploying chaincodes on channels, and configuring the development environment. EOSIO smart contracts are mainly written in C++ and are executed using WebAssembly. They are deployed via the Cleos command-line interface, and they allow for transaction-related operations and interactions via JavaScript/HTML and RPC interfaces. All platforms provide unique deployment procedures and guarantee safe and effective smart contract execution. These studies highlight how crucial it is to combine blockchain technology with frameworks tailored to certain industries in order to improve security, effectiveness, and dependability in a variety of contexts.

EVALUATION AGAINST COMMON ATTACKS

Shah et al.[24] suggested Traffic Control Based on the Maximum Rate of Transactions (TCMRT) as a technique to reduce DDoS attacks by imposing a maximum transaction rate on nodes in the evaluation against typical attacks. When the threshold is surpassed, this method effectively lessens the impact of DDoS attacks by stopping continuous transmissions. On the other hand, it necessitates dynamic threshold modifications and can cause flooding of the communication medium by delaying responses to genuine traffic. Additionally, Wu et al.[25] suggested integrating AI with cloud computing to process massive IoT data and empower ECNs and IoT devices with intelligence to detect and respond to security threats. Deep learning approaches aid in identifying malicious attacks by analysing activity reports. Ad-

vances in differential privacy, homomorphic encryption, and federated learning offer opportunities to protect data privacy alongside blockchain implementation. In order to reduce the computational load on sensor nodes, Vargas et al.[26] presented an IIoT architecture that includes a Collector node for centralising communications, processing data from sensor nodes, and performing Blockchain and Machine Learning (ML) algorithms. For machine learning, the K closest neighbours (KNN) method was selected because of its portability and applicability for threat detection. Regular business operations are maintained without overburdening sensor nodes thanks to centralised computing effort at the collection node. These carefully chosen solutions seek to protect data privacy, preserve system performance, and effectively reduce security threats in industrial IoT contexts.

ENHANCED PRIVACY FEATURES

The assessment assesses the degree to which blockchain platforms facilitate improved privacy features, exposing discrepancies in support between platforms. PETchain's user-centric architecture is highlighted by Javed et al.[27], who point out that users can utilise smart contracts to authorise service providers and manage their data. PETchain protects user privacy by securely decrypting data via trustworthy executors and storing it on distributed storage. In order to protect data privacy, Qashlan et al.[28] concentrate on privacy-preserving techniques in smart homes, utilising edge computing and blockchain. They contrast a private method that uses differential private stochastic gradient descent (DP-SGD) for verifiable differential privacy guarantees with a plain approach that transfers data to the cloud without taking privacy into account. FedCrowd is a blockchain-based, federated, privacy-preserving crowdsourcing platform that was introduced by Farouk et al.[29] In order to overcome the drawbacks of centralised systems, it uses smart contracts and specially designed matching protocols to provide safe job recommendations without requiring the sharing of secret keys. FedCrowd's viability and usability are confirmed by formal security research and prototype implementation, underscoring the platform's potential to improve privacy in crowdsourcing settings.

PERFORMANCE AND FAULT TOLERANCE

Reviewing three researches, the review discusses the fault tolerance and performance of underlying consensus procedures. In their evaluation of consensus protocols in industrial IoT situations, Xiao et al.[30] identify a dearth of platforms that satisfy the strict specifications needed to manage IoT transaction volumes and associated interruptions efficiently. One notable feature of Practical Byzantine Fault Tolerance (PBFT) is its resilience to Byzantine faults without compromising functionality. Based on the Viewstamped Replication (VR) framework, PBFT guarantees consensus amongst trustworthy servers in the face of malevolent attackers, and thorough evaluations support its scalability and dependability. The problem of effective IoT data sharing with Byzantine fault tolerance is addressed by Fu et al.[31]

In addition to specialised algorithms like detectable RAFT (DRAFT) and double-layer parallel BFT (DPBFT), they suggest a revolutionary blockchain consensus transform (BCT) mechanism and provide substantial experimental evidence for their effectiveness. Masood et al.[32] highlight the lack of industrial IoT platforms that are suitable and suggest a data-driven fault-tolerant controller (DD-FTC) to protect Industrial Control Systems (ICS) against failures and integrity assaults. The Neural Network Auto-Regressive eXternal (NNARX) models and Principal Component Analysis (PCA) techniques are integrated by the DD-FTC to detect anomalies and modify parameters to preserve system stability. This comprehensive assessment ensures the selection of platforms capable of sustaining performance amidst escalating IoT transaction volumes and potential disruptions, crucial for the reliability of industrial IoT deployments.

RECENT ADVANCEMENT IN BLOCKCHAIN TECHNOLOGY

A blockchain-based authentication and data sharing system for the Internet of Things was introduced by Fan et al.[33], striking a compromise between security and performance. It does not, however, provide thorough discussion of authentication techniques for improved data transfer security. A patient-centric blockchain framework that addresses immutability and data protection issues on the Hyperledger platform was developed by Singh et al.[34] The framework showed promise but lacked service-based fault tolerance.

Using blockchain technology, Uddin et al.[35] created an eHealth system that integrates the NEAR and FAR processing layers for dependable security and privacy in 5G-based health data management. Through job offloading and blockchain-based consensus techniques, which have been shown to be dependable in real-time health data processing, their patient agent system protects patient privacy. A blockchain authentication and networked identification solution for the Internet of Things was described by Huang et al.[36], who also assessed privacy, performance time, and block speed (Table 1). Their examination of traffic and memory consumption bolsters the reliability and efficiency of the blockchain-based authentication mechanism.

Table 1. Advancements in blockchain in various applications of IoT

Author	Technology	Mode	Methodology	Application
Fan et al.[33]	Scheme based	Private blockchain	Secured data transmission and sharing	IoT
Singh et al.[34]	Smart contract	Private blockchain	Immutability and Authentication	IoT
Uddin et al.[35]	Consensus protocol	Architecture blockchain	Monitoring and managing data	Healthcare
Huang et al.[36]	Consensus protocol	System blockchain	Improves authentication	IoT

CHALLENGES AND FUTURE SCOPE

Implementing blockchain-based Internet of Things applications presents a number of challenges and trends in the future. The gigabytes of data produced by IoT sensors in real time are too much for current blockchain implementations to handle; therefore scalability is still a major challenge[37]. Another difficulty is interoperability, especially when it comes to cost control, data trading, and resource sharing. Consensus methods need a significant amount of energy and computational resources; hence they must be improved in order to increase system performance and efficiency[38]. Despite their potential, smart contracts have problems with integration and scalability, particularly when it comes to efficiently allocating computational jobs and gaining access to real-world data sources. Identity management creates issues in providing secure ownership and authentication, despite blockchain's power to deliver immutable records and digital evidence[39]. Consensus protocol attacks, smart contract vulnerabilities, privacy protection, and legal uncertainty are only a few of the security, legal, and regulatory issues that demand careful thought and mitigating techniques[40]. In order to fully utilise blockchain-enabled Internet of Things applications and promote innovation and confidence in newly developing digital ecosystems, it will be imperative to address these issues.

CONCLUSIONS

The review underscores the critical necessity for robust blockchain solutions specifically designed to address the intricate challenges posed by IoT applications, particularly within industrial contexts. Recognising the inherent complexities and vulnerabilities within industrial IoT environments, the conclusion highlights the imperative for tailored blockchain solutions that can effectively address these challenges. To this end, the review offers insightful recommendations aimed at guiding the selection and implementation of blockchain solutions to safeguard the integrity, security, and efficiency of IoT systems operating within industrial settings.

Firstly, the review emphasises the importance of thoroughly evaluating and selecting blockchain platforms that exhibit robustness in handling the unique demands of industrial IoT scenarios. Platforms should possess inherent capabilities to ensure data integrity, resilience against cyber threats, and efficient transaction processing, all while maintaining high levels of performance. Additionally, the review advocates for the adoption of consensus protocols, such as Practical Byzantine Fault Tolerance (PBFT), that have demonstrated effectiveness in tolerating Byzantine failures while sustaining optimal performance levels. By leveraging consensus mechanisms like PBFT, industrial IoT systems can maintain operational continuity even in the face of malicious attacks or network disruptions.

Furthermore, the review underscores the significance of incorporating advanced security measures within blockchain implementations for industrial IoT

applications. This includes implementing cryptographic techniques to safeguard data confidentiality and integrity, as well as deploying robust authentication and access control mechanisms to prevent unauthorised access to sensitive IoT data. Additionally, the review highlights the importance of regular security audits and vulnerability assessments to proactively identify and mitigate potential security risks within blockchain-enabled IoT systems.

In conclusion, the review emphasises that successful deployment of blockchain solutions in industrial IoT environments hinges upon careful consideration of platform robustness, consensus protocol efficacy, and security measures implementation. By adhering to the provided recommendations and selecting blockchain solutions tailored to the unique requirements of industrial IoT applications, organisations can effectively enhance the integrity, security, and efficiency of their IoT systems, thereby ensuring seamless operation and mitigating potential risks in industrial settings.

REFERENCES

1. X. XU, Z. ZENG, S. YANG, H. SHAO: A Novel Blockchain Framework for Industrial IoT Edge Computing. Sensors, **20** (7), 2061 (2020).
2. T. KUMAR, E. HARJULA, M. EJAZ, A. MANZOOR, P. PORAMBAGE et al.: BlockEdge: Blockchain-edge Framework for Industrial IoT Networks. IEEE Access, **8**, 154166 (2020).
3. X. L. LIU, W. M. WANG, H. GUO, A. V. BARENJI, Z. LI, G. Q. HUANG: Industrial Blockchain Based Framework for Product Lifecycle Management in Industry 4.0. Robot CIM-Int Manuf, **63**, 101897 (2020).
4. G. WANG: SOK: Applying Blockchain Technology in Industrial Internet of Things. Cryptology ePrint Archive, (2021).
5. R. L. KUMAR, F. KHAN, S. KADRY, S. RHO: A Survey on Blockchain for Industrial Internet of Things. Alex Eng J, **61** (8), 6001 (2022).
6. I. MISTRY, S. TANWAR, S. TYAGI, N. KUMAR: Blockchain for 5G-enabled IoT for Industrial Automation: a Systematic Review, Solutions, and Challenges. Mechanical Systems and Signal Processing (MSSP), **135**, 106382 (2020).
7. Q. WANG, X. ZHU, Y. NI, L. GU, H. ZHU: Blockchain for the IoT and Industrial IoT: a Review. IoT, **10**, 100081 (2020).
8. A. R. RAO, D. CLARKE: Perspectives on Emerging Directions in Using IoT Devices in Blockchain Applications. IoT, **10**, 100079 (2020).
9. M. A. UDDIN, A. STRANIERI, I. GONDAL, V. BALASUBRAMANIAN: A Survey on the Adoption of Blockchain in IoT: Challenges and Solutions. Blockchain: Res Appl, **2** (2), 100006 (2021).
10. S. SAXENA, B. BHUSHAN, M. A. AHAD: Blockchain Based Solutions to Secure IoT: Background, Integration Trends and a Way Forward. J Netw Comput Appl, **181**, 103050 (2021).
11. S. SINGH, A. S. HOSEN, B. YOON: Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network. IEEE Access, **9**, 13938 (2021).
12. C. ROY, S. MISRA, S. PAL: Blockchain-enabled Safety-as-a-service for Industrial IoT Applications. IEEE Internet of Things Magazine (IoTM), **3** (2), 19 (2020).
13. S. K. DWIVEDI, P. ROY, C. KARDA, S. AGRAWAL, R. AMIN:. Blockchain-based Internet of Things and Industrial IoT: a Comprehensive Survey. Secur Commun Netw, **2021**, 1 (2021).

14. N. MALIK, K. ALKHATIB, Y. SUN, E. KNIGHT, Y. JARARWEH: A Comprehensive Review of Blockchain Applications in Industrial Internet of Things and Supply Chain Systems. Appl Stoch Models Bus Ind, **37** (3), 391 (2021).
15. L. YANG, W. ZOU, J. WANG, Z. TANG: EdgeShare: a Blockchain-based Edge Data-sharing Framework for Industrial Internet of Things. Neurocomputing, **485**, 219 (2022).
16. J. LI, A. MAITI, M. SPRINGER, T. GRAY: Blockchain for Supply Chain Quality Management: Challenges and Opportunities in Context of Open Manufacturing and Industrial Internet of Things. Int J Comput Integr Manuf, **33** (12), 1321 (2020).
17. T. GEBREMICHAEL, L. P. LEDWABA, M. H. ELDEFRAWY, G. P. HANCKE, N. PEREIRA et al.: Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges. IEEE Access, **8**, 152351 (2020).
18. M. SERROR, S. HACK, M. HENZE, M. SCHUBA, K. WEHRLE: Challenges and Opportunities in Securing the Industrial Internet of Things. IEEE Trans Ind Inform, **17** (5), 2985 (2020).
19. P. KRISHNAN, K. JAIN, K. ACHUTHAN, R. BUYYA: Software-defined Security-by-contract for Blockchain-enabled MUD-aware Industrial IoT Edge Networks. IEEE Trans Ind Inform, **18** (10), 7068 (2021).
20. R. B. URIARTE, H. ZHOU, K. KRITIKOS, Z. SHI, Z. ZHAO, R. De NICOLA: Distributed Service-Level Agreement Management with Smart Contracts and Blockchain. Concurr Comput: Pract Exp, **33** (14), e5800 (2021).
21. A. A. KHAN, A. A. WAGAN, A. A. LAGHARI, A. R. GILAL, I. A. AZIZ, B. A. TALPUR: BIOMT: A State-of-the-Art Consortium Serverless Network Architecture for Healthcare System Using Blockchain Smart Contracts. IEEE Access, **10**, 78887 (2021).
22. S. N. G. GOURISETTI, D. J. SEBASTIAN-CARDENAS, B. BHATTARAI, P. WANG, S. WIDERGREN et al.: Blockchain Smart Contract Reference Framework and Program Logic Architecture for Transactive Energy Systems. Appl Energy, **304**, 117860 (2021).
23. L. ZHANG, J. LI, L. L. JI, Y. SUN: A Survey of Application Research Based on Blockchain Smart Contract. Wirel Netw, **28** (2), 635 (2022)
24. Z. SHAH, I. ULLAH, H. LI, A. LEVULA, K. KHURSHID: Blockchain Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things (IoT): a Survey. Sensors, **22** (3), 1094 (2022).
25. Y. WU, H. N. DAI, H. WANG: Convergence of Blockchain and Edge Computing for Secure and Scalable IIoT Critical Infrastructures in Industry 4.0. IEEE Internet Things J, **8** (4), 2300 (2020).
26. H. VARGAS, C. LOZANO-GARZON, G. A. MONTOYA, Y. , DONOSO: Detection of Security Attacks in Industrial IoT Networks: a Blockchain and Machine Learning Approach. Electronics, **10** (21), 2662 (2021).
27. I. T. JAVED, F. ALHARBI, T. MARGARIA, N. CRESPI, K. N. QURESHI: PETchain: a Blockchain-based Privacy Enhancing Technology. IEEE Access, **9**, 41129 (2021).
28. A. QASHLAN, P. NANDA, X. HE, M. MOHANTY: Privacy-preserving Mechanism in Smart Home Using Blockchain. IEEE Access, **9**, 103651 (2021).
29. A. FAROUK, A. ALAHMADI, S. GHOSE, A. MASHATAN: Blockchain Platform for Industrial Healthcare: Vision and Future Opportunities. Comput Commun, **154**, 223 (2020).
30. Y. XIAO, N. ZHANG, W. LOU, Y. T HOU: A Survey of Distributed Consensus Protocols for Blockchain Networks. IEEE Commun Surv Tut, **22** (2), 1432 (2020).
31. J. FU, L. ZHANG, L. WANG, F. LI: BCT: an Efficient and Fault Tolerance Blockchain Consensus Transform Mechanism for IoT. IEEE Internet Things J, **10** (14), 12055 (2021).
32. A. B. MASOOD, A. HASAN, V. VASSILIOU, M. LESTAS: A Blockchain-based Data-driven Fault-tolerant Control System for Smart Factories in Industry 4.0. Comput Commun, **204**, 158 (2023).

33. Q. FAN, J. CHEN, L. J. DEBORAH, M. LUO: A Secure and Efficient Authentication and Data Sharing Scheme for Internet of Things Based on Blockchain. Journal of Systems Architecture (JSA), **117**, 102112 (2021).
34. A. P. SINGH, N. R. PRADHAN, A. K. LUHACH, S. AGNIHOTRI, N. Z. JHANJHI et al.: A Novel Patient-centric Architectural Framework for Blockchain-enabled Healthcare Applications. IEEE Trans Industr Inform, **17** (8), 5779 (2020).
35. M. A. UDDIN, A. STRANIERI, I. GONDAL, V. BALASUBRAMANIAN: Blockchain Leveraged Decentralized IoT eHealth Framework. Internet of Things, **9**, 100159 (2020).
36. J. C. HUANG, M. H. SHU, B. M. HSU, C. M. HU: Service Architecture of IoT Terminal Connection Based on Blockchain Identity Authentication System. Comput Commun, **160**, 411 (2020).
37. P. K. SHARMA, N. KUMAR, J. H. PARK: Blockchain Technology toward Green IoT: Opportunities and Challenges. IEEE Network, **34** (4), 263 (2020).
38. A. SINGH, G. KUMAR, R. SAHA, M. CONTI, M. ALAZAB, R. THOMAS: A Survey and Taxonomy of Consensus Protocols for Blockchains. Journal of Systems Architecture (JSA), **127**, 102503 (2022).
39. Y. LIU, D. HE, M. S. OBAIDAT, N. KUMAR, M. K. KHAN, K. K. R. CHOO: Blockchain-based Identity Management Systems: a Review. J Netw Comput Appl, **166**, 102731 (2020).
40. X. XIAO, Z. YU, K. XIE, S. GUO, A. XIONG, Y. YAN: A Multi-blockchain Architecture Supporting Cross-blockchain Communication. In: Proceedings of the 6th International Conference 'Artificial Intelligence and Security', ICAIS 2020, Hohhot, China, July 17–20, 2020, Part II 6, 592–603, 2020.

Received 2 April 2024
Accepted 5 July 2024